# SUMMARY TABLE FOR: "Internet PKI, X.509 Certificate and CRL Profile," draft-ietf-pkix-ipki-part1-07.txt, March 25, 1998

## 9 JUNE 1998

*Prepared by:*

**Center for Standards**
**Defense Information Systems Agency**

This supercedes version dated 7 May 1998 and all earlier versions.

This Page left intentionally blank.

## Disclaimer

Persons and organizations use this document at their own risk.

This document is for information only. If there is any conflict between this document and the source document, the source document takes precedence.

The U. S. Federal Government does NOT provide any guarantee as to the accuracy of this document. This document is NOT a request for proposal, a request for bid, or a modification to any contract currently held with the U. S. Federal Government.

Distribution of this document is unlimited.

## Acronyms

| | |
|---|---|
| CA | - Certifying Authority |
| CPS | – Certification Practice Statement |
| DH | - Diffie-Hellman |
| DN | - Distinguished Name |
| DSA | - Digital Signature Authority |
| MD | - Message Digest |
| OCSP | – On-line Certificate Status Protocol |
| OID | – Object Identifier |
| PCA | - Policy Certification Authorities |
| PEM | - Privacy Enhanced Mail |
| PKIXLDAP | - Internet PKI, Operational Protocols - LDAPv2 |
| PKIXOCSP | - Internet PKI, Online Certificate Status Protocol |
| RSA | - Rivest, Shamir, and Adelman |
| TBS | - To Be Signed |
| URI | - Uniform Resource Identifier |

This Page left intentionally blank.

STATUS CODES: M – MANDATORY, O – OPTIONAL, C - CONDITIONAL

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| 3.1 | **X.509 VERSION 3 CERTIFICATE** | M | ref. X509 - 97 |
| | CA digitally signs each certificate | M | |
| | Certificate has a limited valid lifetime | M | |
| | CA maintains certificate status during validity period | M | ref. 4.1.2.5 |
| | Support of directory access control | M | v(2), DAP? |
| | Support for additional extension fields | M | v(3) |
| | Standard extensions: | M | v(3) |
| | Additional subject identification information | O | |
| | Key attribute information | O | |
| | Policy information | O | |
| | Certification path constraints | O | |
| | Interoperable over WWW, electronic mail, and IPSEC applications | M | HTTP, SMTP, SMIME, SSL/TLS |
| 3.2 | **CERTIFICATION PATHS AND TRUST** | M | |
| | Support of certification paths | M | |
| | Start with public key of CA within user's own domain | O | |
| | Start at the top of a hierarchy of CAs | O | |
| | Name constraints imposed | O | |
| | Path acceptance based on the contents of the certificates (policy extensions and mappings) | O | |
| 3.3 | **REVOCATION** | M | |
| | Certificate Revocation List (CRL) | O | ref. X.509 |
| | CA updates a CRL on a regularly periodic basis | M | |
| | CA signs CRL | M | |
| | CRL is dated | M | |
| | CRL available in a public repository | M | |
| | Revoked certificates are identified by their certificate serial number | M | |
| | Certificate–using system checks most recently-issued CRL before accepting a certificate | M | |
| | Certificates are entered into the CRL upon revocation | M | |
| | CRL entries removed when the certificate expiration date is reached | O | |
| | Support of X.509 CRL v2 format | O | |
| | Partition population of certificates for one CA per one CRL distribution point | M | |
| | CRL distribution points handles those revocations related to a specific reason | O | |
| | On-line method of revocation notification | O | Ref. [PKIXOCSP] Reduces latency between revocation and next issue of CRL |
| | Queries to on-line service reflect latest certificate revocations | M | |
| | Trust between the certificate validator and on-line validation service | M | |
| 3.4 | **OPERATIONAL PROTOCOLS** | M | ref. [PKIXLDAP], [PKIXFTP], [PKIXOCSP] |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Means to deliver certificates and CRLs to client systems | M | |
| | Variety of different means of delivery: | M | |
| | E-mail (MIME) | M | |
| | http | M | |
| | X.500 | M | |
| | WHOIS++ | M | |
| 3.5 | **MANAGEMENT PROTOCOLS** | M | ref. [PKIXMGT] |
| | Support interactions between PKI components | M | Either on-line, off-line or a mix of both protocols |
| | User registration with the CA | M | |
| | Key material initialization | M | |
| | CA issues a certificate for a user's public key | M | |
| | User key backup/recovery | O | |
| | User key pair/certificate update | M | |
| | Revocation request | M | |
| | Cross-certification | M | |
| 4 | **CERTIFICATE AND CERTIFICATE EXTENSIONS PROFILE** | M | ref. X.509 - 97, 1988 ASN.1 Syntax |
| 4.1 | **BASIC CERTIFICATE FIELDS** | M | |
| 4.1.1 | **Certificate** ::= SEQUENCE | M | |
| 4.1.1.1 | tbsCertificate TBSCertificate | M | ref. 4.1.2 |
| 4.1.1.2 | signatureAlgorithm | M | |
| | AlgorithmIdentifier ::= SEQUENCE | M | Algorithm used by CA to sign certificate |
| | algorithm OID | M | |
| | Supported signature algorithms | M | ref. 7.2 |
| | Same algorithm as identified in signature field of TBSCertificate | M | ref. 4.1.2.3 |
| | parameters NULL | M | |
| 4.1.1.3 | signature | M | CA certifies the validity of tbscertificate information |
| | CA generated | M | ref. 7.2 for details on each supported algorithm |
| | ASN.1 DER encoded TBSCertificate is inputted into a one-way hash | M | ref. X.208 – 88, a TLV encoding for each element |
| | Hash output is encrypted to form signed quantity | M | |
| | Signed quantity is ASN.1 encoded as a BIT STRING | M | |
| 4.1.2 | **TBSCertificate** ::= SEQUENCE | M | |
| 4.1.2.1 | **Version** INTEGER (0,1,2) | M | v1(0), v2(1), v3(2) Generation of v2 certificates not expected of IPKI implementations |
| | Value is 2 when extensions are used | M | |
| | Value is 1 when no extensions, but a UniqueIdentifier present | M | Backward compatibility requirement? **Apparent conflict with basic syntax shown in 4.1. That seems to imply a value of 2 is also permitted.** |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Field omitted if only basic fields are used | M | Backward compatibility requirement? Only if receiving a v(1) cert? |
| | Field omitted is default | M | Backward compatibility requirement? **v(1) certificate is default?** |
| | All values accepted by receiving implementations | O | |
| | Value 2 is accepted by receiving implementations | M | |
| 4.1.2.2 | **Serial Number** INTEGER | M | Issuer name and serial number identify a unique certificate |
| | Unique for each certificate issued by a CA | M | |
| 4.1.2.3 | **Signature** | O | |
| | AlgorithmIdentifier ::= SEQUENCE | M | Algorithm used by CA to sign certificate |
| | algorithm OID | M | |
| | Supported signature algorithms | M | ref. 7.2 |
| | Same algorithm as identified in signatureAlgorithm | M | ref. 4.1.1.2 |
| | parameters NULL | M | |
| 4.1.2.4 | **Issuer Name** | M | CA that signed and issued certificate |
| | X.500 distinguished name | O | |
| | issuerAltName extension present | O | |
| | X.501 type Name | M | X.500 attribute types recommended |
| | RelativeDistinguishedName | M | |
| | AttributeType ::= OID | M | |
| | AttributeValue ::= ANY | M | determined by AttributeType |
| | DirectoryString ::= CHOICE | O | |
| | printableString | C | FIRST CHOICE |
| | bmpString | C | SECOND CHOICE |
| | utf8String | C | THIRD CHOICE |
| | universalString | C | FOURTH CHOICE |
| | teletexString | O | USE UNSPECIFIED |
| | NULL | O | |
| | issuerAltName extension present | M | |
| | Critical | M | |
| 4.1.2.5 | **Validity** | M | The time interval that the CA warrants it will maintain information about the certificate status. |
| | notBefore | M | First date certificate is valid |
| | CAs use utcTime through 2049 | M | ref. 4.1.2.5.1 |
| | Values expressed in Zulu | M | |
| | Values include seconds | M | |
| | Interpretation of YY field by certificate users | M | |
| | >= 50 then 19YY | M | Shouldn't appear if CA conforms to specification |
| | < 49 then 20YY | M | |
| | CAs use generalTime 2050 or after | M | ref. 4.1.2.5.2 |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Values expressed in Zulu | M | |
| | Values include seconds | M | |
| | Values not include fractional seconds | M | |
| | notAfter | M | Last date certificate is valid |
| | CAs use utcTime through 2049 | M | ref. 4.1.2.5.1 |
| | Values expressed in Zulu | M | |
| | Values will include seconds | M | |
| | Interpretation of YY field by certificate users | M | |
| | >= 50 then 19YY | M | Shouldn't appear if CA conforms to specification |
| | < 49 then 20YY | M | |
| | CAs use generalTime 2050 or after | M | ref. 4.1.2.5.2 |
| | Values expressed in Zulu | M | |
| | Values will include seconds | M | |
| | Values not include fractional seconds | M | |
| 4.1.2.6 | **Subject Name** | M | Identifies end entity associated with the public key in the certificate |
| | X.500 distinguished name | O | |
| | subjectAltName extension present | O | |
| | Unique for each subject entity certified by a CA defined in the issuer name field | M | |
| | CA may issue more than one certificate with the same DN to subject | O | |
| | X.501 type Name | M | ref. 4.1.2.4<br>X.500 attribute types recommended |
| | RelativeDistinguishedName | M | |
| | AttributeType ::= OID | M | |
| | AttributeValue ::= ANY | M | determined by AttributeType |
| | DirectoryString ::= CHOICE | O | |
| | printableString | C | FIRST CHOICE |
| | bmpString | C | SECOND CHOICE |
| | utf8String | C | THIRD CHOICE |
| | universalString | C | FOURTH CHOICE |
| | teletexString | O | USE UNSPECIFIED |
| | NULL | O | |
| | subjectAltName extension present | M | |
| | Critical | M | |
| 4.1.2.7 | **Subject Public Key Info** ::= SEQUENCE | M | Carries the public key & identifies the algorithm with which it is used |
| | AlgorithmIdentifier ::= SEQUENCE | M | ref. 4.1.1.2 |
| | algorithm OID | M | |
| | Supported algorithms | M | ref. 7.3 |
| | parameters NULL | M | |
| | subjectPublicKey ::= BIT STRING | M | Encoding methods for key materials, ref. 7.3 |
| 4.1.2.8 | **Unique Identifiers** | O | NOT RECOMMENDED<br>Permits reuse of subject and/or issuer names |
| | issuerUniqueID | O | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | subjectUniqueID | O | |
| | CAs can generate certificates with unique identifiers | O | |
| | Application can parse unique identifiers and make comparisons | O | |
| 4.1.2.9 | **Extensions** | O | Format and content, ref. 4.2 |
| | Version value is 2 | M | v(3) |
| | extensions ::= SEQUENCE SIZE (1..MAX) OF | M | ref. 4.1 |
| | extension ::= SEQUENCE | M | |
| | extnID OID | M | |
| | critical BOOLEAN | M | |
| | Default FALSE | M | |
| | extnValue OCTET STRING | M | |
| 4.2 | **CERTIFICATE EXTENSIONS** | | For associating additional attributes with users or public keys (ref. 4.2.1), managing certificate hierarchy (ref. 4.2.1.6,.10,.11,.12), and managing CRL distribution (ref. 4.2.1.13) |
| | Definition of private certificate extensions | O | |
| | Restrict critical private certificate extensions | O | RECOMMENDED |
| | Applications reject certificates if critical extension not recognized | M | |
| | Applications reject certificates if non-critical extension not recognized | O | |
| | Only one instance of each extension type | M | |
| | General Syntax | M | |
| | extnID extension OID | M | |
| | extnvalue OCTET STRING (ASN.1 encoded) | M | |
| | critical BOOLEAN | O | |
| | default FALSE | M | |
| | CA support of authority key identifier extension | O | RECOMMENDED, ref. 4.2.1.1, |
| | CA support of subject key identifier extension | O | ref. 4.2.1.2, |
| | CA support of key usage extension | M | ref. 4.2.1.3 |
| | CA support of private key usage period extension | O | NOT RECOMMENDED, ref. 4.2.1.4 |
| | CA support of certificate policies extension | M | ref. 4.2.1.5 |
| | CA support of policy mappings extension | O | ref. 4.2.1.6 |
| | CA issue certificates with NULL subject field | C | |
| | CA support of subject alternate name | M | ref. 4.2.1.7 |
| | CA issue certificates with NULL issuer field | C | |
| | CA support of issuer alternate name | M | ref. 4.2.1.8 |
| | CA support of subject directory attributes extension | O | NOT RECOMMENDED, ref. 4.2.1.9 |
| | CA support of basic constraint extension | M | ref. 4.2.1.10 |
| | CA support of name constraints extension | O | ref. 4.2.1.11 |
| | CA support of policy constraints extension | O | ref. 4.2.1.12 |
| | CA support of CRL distribution points extension | O | RECOMMENDED, ref. 4.2.1.13 |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | CA support of extended key usage field extension | O | ref. 4.2.1.14 |
| | CA support of unspecified extensions | O | |
| | Marking as critical | O | NOT RECOMMENDED |
| | Application support for authority key identifier | O | RECOMMENDED, ref. 4.2.1.1 |
| | Application support for subject key identifier | O | RECOMMENDED, ref. 4.2.1.2 |
| | Application recognize criticality of key usage | M | NOT RECOMMENDED, ref. 4.2.1.3 |
| | Application support of private key usage period | O | ref. 4.2.1.4 |
| | Application recognize criticality of certificate policies | M | ref. 4.2.1.5 |
| | Application support of policy mapping extension | O | ref. 4.2.1.6 |
| | Application recognize criticality of subject alternative name | M | ref. 4.2.1.7 |
| | Application recognize criticality of issuer alternative name | M | ref. 4.2.1.8 |
| | Application support of subject directory attribute | O | NOT RECOMMENDED, ref. 4.2.1.9 |
| | Application recognize criticality of basic constraints | M | ref. 4.2.1.10 |
| | Application recognize criticality of name constraints | M | ref. 4.2.1.11 |
| | Application recognize criticality of policy constraints | M | ref. 4.2.1.12 |
| | Application support for CRL distribution points | O | RECOMMENDED, ref. 4.2.1.13 |
| | Application recognize criticality of extended key usage | M | ref. 4.2.1.14 |
| | Application support for authority information access | O | RECOMMENDED, ref. 4.2.2.1 |
| 4.2.1 | **STANDARD EXTENSIONS** | M | ref. x.509 |
| | Extensions defined under id-ce arc | M | |
| 4.2.1.1 | **Authority Key Identifier OID ::= {id-ce 35}** | O | RECOMMENDED. Identifies the public key to the private key that signed the certificate. |
| | Non-critical | M | |
| | Use when issuer has multiple signing keys | O | Multiple concurrent key pairs or due to a changeover. |
| | SEQUENCE | M | |
| | **keyIdentifier OCTET STRING** | O | RECOMMENDED. Same as in CRL signer's certificate. |
| | Subject key identifier in issuer's certificate | M | |
| | If authorityCertIssuer and authorityCertSerialNumber are NULL fields | M | |
| | authorityCertIssuer | O | Alternative to keyIdentifier |
| | Issuer's name | M | ref. 4.1.2.4 |
| | X.500 distinguished name | O | |
| | issuerAltName extension present | O | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | X.501 type Name | M | X.500 attribute types recommended |
| | RelativeDistinguishedName | M | |
| | AttributeType OID | M | |
| | AttributeValue | M | determined by AttributeType |
| | DirectoryString | O | |
| | printableString | C | FIRST CHOICE |
| | bmpString | C | SECOND CHOICE |
| | utf8String | C | THIRD CHOICE |
| | universalString | C | FOURTH CHOICE |
| | teletexString | O | USE UNSPECIFIED |
| | NULL | O | |
| | issuerAltName extension present | M | |
| | Critical | M | |
| | Present if authorityCertSerialNumber present | M | |
| | Absent if authorityCertSerialNumber absent | M | |
| | authorityCertSerialNumber INTEGER | O | Alternative to keyIdentifier |
| | Issuer's serial number | M | ref. 4.1.2.2 |
| | Present if authorityCertIssuer present | M | |
| | Absent if authorityCertIssuer absent | M | |
| 4.2.1.2 | **Subject Key Identifier** | O | Identifies public key used in an application |
| | Non-critical | M | |
| | Public key identifier needed but absent from certificate | M | |
| | SHA-1 hash of BIT STRING subjectPublicKey value (excluding tag and length) in the certificate | M | |
| 4.2.1.3 | **Key Usage OID ::= {id-ce 15}** | M | Defines the purpose of the key in the certificate. Restricts the operations the key can be used on. |
| | Critical | O | RECOMMENDED |
| | Syntax BIT STRING | M | |
| | digitalSignature (0) | O | Subject public key used to verify for other than non-repudiation, certificate and CRL signature |
| | nonRepudiation (1) | O | Subject public key used to verify digital signature |
| | Not used for certificate and CRL signing | M | |
| | keyEncipherment (2) | O | Subject public key used for key transport |
| | dataEncipherment (3) | O | Subject public key used to encipher user data |
| | Not used for enciphering cryptographic keys | M | |
| | keyAgreement (4) | O | Subject public key used for key agreement |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | keyCertSign (5) | O | Subject public key used to verify CA signature on certificate |
| | Asserted with CA certificates only | M | |
| | cRLSign (6) | O | Subject public key used to verify CA signature on CRLs |
| | encipherOnly (7) | O | |
| | Asserted and keyAgreement bit set | M | Subject public key used to encipher data while performing key agreement |
| | Asserted and keyAgreement bit not set | O | Meaning unspecified |
| | decipherOnly (8) | O | |
| | Asserted and keyAgreement bit set | M | Subject public key used to decipher data while performing key agreement |
| | Asserted and keyAgreement bit not set | O | Meaning unspecified |
| | Bit combinations unrestricted | M | |
| | Bit settings for particular algorithms | M | ref. 7.3 |
| | Purpose redefined in extended key usage field extension | O | ref. 4.2.1.14 |
| | Critical extended key usage field extension present | C | ref. 4.2.1.14 |
| | Process both fields | M | |
| | Certificate use consistent with both fields | M | |
| | Purposes inconsistent, certificate is rejected | M | |
| 4.2.1.4 | **Private Key Usage Period OID ::= {id-ce 16}** | O | NOT RECOMMENDED Allows certificate issuer to specify a different validity period for the issuer's private key than the certificate |
| | Non-critical | M | |
| | Use with digital signature keys | M | ref. 4.2.1.3 |
| | Syntax | | |
| | notBefore GeneralizedTime | O | First date certificate is valid, ref. 4.1.2.5.2 |
| | Values expressed in Zulu | M | |
| | Values include seconds | M | |
| | Values not include fractional seconds | M | |
| | notAfter GeneralizedTime | O | Last date certificate is valid, ref. 4.1.2.5.2 |
| | Values expressed in Zulu | M | |
| | Values will include seconds | M | |
| | Values not include fractional seconds | M | |
| | Associated private key signs objects only between times specified | O | |
| | Conformant CAs issue certificates with one time component present | M | |
| | Conformant CAs not issue certificates using this extension | M | |
| 4.2.1.5 | **Certificate Policies OID ::= {id-ce 32}** | M | The policy under which the certificate was issued and can be used. |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Support a sequence of one or more policy information terms | M | |
| | OID | M | RECOMMENDED |
| | Optional qualifiers | O | How to obtain CA rules |
| | No change to policy definitions | M | |
| | CPS Pointer qualifier | O | |
| | URI pointer to CPS [IA5String] | M | |
| | User Notice qualifier | O | Display to relying party when a certificate is used |
| | Application display all user notices in all certificates of certification path | O | |
| | Don't display duplicates | O | |
| | Only the lowest-level certificate per issuer in certification path contain a user notice | O | RECOMMENDED |
| | noticeRef field | O | |
| | Organization name [IA5String] | M | |
| | Identifies numbered text statement [SEQUENCE OF INTEGER] | M | Prepared by named organization |
| | Application maintains notice file | O | |
| | Contains current set of notices per issuing organization | M | |
| | Notice text extracted from this file and displayed | M | |
| | Support multilingual statements | O | |
| | explicitText field | O | |
| | Include text statement with certificate | M | |
| | 200 character string maximum | M | |
| | VisibleString | O | |
| | BMPString | O | |
| | UTF8String | O | |
| | Both fields present | O | |
| | Display text in noticeRef field | O | |
| | Else display explicitText | C | |
| | Application has specific policy requirements | O | |
| | Maintains a list of policies they will accept | M | |
| | Compare extension OIDs against list | M | |
| | If critical reject certificate if unable to interpret extension | M | |
| | Application has no specific policy requirements | O | |
| | Accept any valid certificate | O | |
| 4.2.1.6 | **Policy Mappings OID ::= {id-ce 33}** | O | Used in CA certificates |
| | Lists one or more pairs of OIDs | M | Tells issuing CA's users which policies associated with subject CA compare to ones they accept |
| | Syntax | M | |
| | issuerDomainPolicy | M | The issuing CA's policy |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | subjectDomainPolicy | M | What the issuing CA considers the equivalent policy of the subject CA |
| | Non-critical | M | |
| 4.2.1.7 | **Subject Alternative Name OID ::= {id-ce 17}** | CA – C<br>App - M | Binds additional identities to certificate subject |
| | CA verifies all parts of subject alternative name | M | |
| | Subject identity only appears in this extension | C | ref. 4.1.2.6 |
| | Subject name field is empty | M | |
| | Critical | M | |
| | Extension present | C | |
| | At least one entry present | M | Client behavior on encountering empty field UNSPECIFIED |
| | Syntax | M | |
| | otherName | O | |
| | OID | M | |
| | related value | M | |
| | rfc822Name | O | |
| | IA5String | M | |
| | Wildcard characters prohibited | M | |
| | Host names only | M | |
| | dNSName | O | |
| | IA5String | M | |
| | Wildcard characters prohibited | M | |
| | Subject is a subnet or a collection of hosts | M | |
| | x400Address | O | |
| | ORAdress | M | |
| | dierctoryName | O | |
| | ediPartyName | O | |
| | nameAssigner | O | |
| | partyName | M | |
| | URI | O | Response to use of other protocol, relative pathname, or omission of host UNSPECIFIED |
| | Points to a sequence of certificates issued by CA to subject | M | |
| | Absolute pathname to a host | M | |
| | ftp | O | |
| | anonymous | M | |
| | http | O | |
| | ldap | O | ref. RFC1778 |
| | mailto | O | ref. RFC1783 |
| | mail response containing subject's certificate | M | |
| | Points to a sequence of certificates issued by CA to other CAs | O | |
| | Absolute pathname to a host | M | |
| | ftp | O | |
| | anonymous | M | |
| | http | O | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | ldap | O | ref. RFC1778 |
| | mailto | O | ref. RFC1783 |
| | mail response containing subject's certificate | M | |
| | IA5String | M | |
| | wildcard character prohibited | M | |
| | iPAddress | O | |
| | OCTET STRING | M | |
| | network byte order | M | ref. RFC791 |
| | each octet LSB is the LSB of the corresponding of network address | M | |
| | IPv4 length 4 octets | M | ref. RFC791 |
| | IPv6 length 16 octets | M | ref. RFC1883 |
| | registerID | O | |
| | OID | M | |
| | Local name definitions permitted | O | |
| | Multiple instances of a name | O | |
| | Multiple name forms | O | |
| | Additional identifier in subject DN | O | NOT PREFERRED |
| | Use of name constraints | O | ref. 4.2.1.11 |
| 4.2.1.8 | **Issuer Alternative Name** | CA – C<br>App - M | Binds additional identities to certificate issuer |
| | Only alternative name form present | C | |
| | Issuer name field is empty | M | |
| | Extension is used | M | |
| | At least one entry present | M | Client behavior on encountering empty field UNSPECIFIED |
| | Extension is critical | M | |
| | Syntax | M | 4.2.1.7 |
| | otherName | O | |
| | OID | M | |
| | related value | M | |
| | rfc822Name | O | |
| | IA5String | M | |
| | Wildcard character prohibited | M | |
| | dNSName | O | |
| | IA5String | M | |
| | Wildcard character prohibited | M | |
| | x400Address | O | |
| | ORAdress | M | |
| | dierctoryName | O | |
| | ediPartyName | O | |
| | nameAssigner | O | |
| | partyName | M | |
| | URI | O | ref. 4.2.1.7 |
| | Points to a ASN.1 sequence of certificates issued to CA | M | |
| | Absolute pathname to a host | M | |
| | ftp | O | |
| | anonymous | M | |
| | http | O | |
| | ldap | O | ref. RFC1778 |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | mailto | O | ref. RFC1783 |
| | mail response containing subject's certificate | M | |
| | Points to a ASN.1 sequence of certificates issued to other CAs | O | |
| | Absolute pathname to a host | M | |
| | ftp | O | |
| | anonymous | M | |
| | http | O | |
| | ldap | O | ref. RFC1778 |
| | mailto | O | ref. RFC1783 |
| | mail response containing subject's certificate | M | |
| | IA5String | M | |
| | Wildcard character prohibited | M | |
| | iPAddress | O | |
| | OCTET STRING | M | |
| | network byte order | M | ref. RFC791 |
| | each octet LSB is the LSB of the corresponding of network address | M | |
| | IPv4 length 4 octets | M | ref. RFC791 |
| | IPv6 length 16 octets | M | ref. RFC1883 |
| | registerID | O | |
| | OID | M | |
| | Multiple instances of a name | O | |
| | Multiple name forms | O | |
| | Use of name constraints | O | ref. 4.2.1.11 |
| 4.2.1.9 | **Subject Directory Attributes** | O | |
| | Local environment use | O | |
| | Non-critical | M | |
| 4.2.1.10 | **Basic Constraints OID ::= {id-ce 19}** | M | Identifies the certificate subject as a CA and how deep a certificate path exists beyond it. |
| | SEQUENCE | M | |
| | cA BOOLEAN | M | |
| | default FALSE | M | |
| | pathLenConstraint field ignored | M | |
| | TRUE – subject of the certificate is a CA | O | |
| | pathLenConstraint field checked | M | |
| | pathLenConstraint | O | |
| | Value = 0, an EE certificate follows | M | |
| | Value > 0 | M | Max number of certificates along certification path that may follow this CA certificate |
| | Not present, no limit to certification path | M | |
| | Critical for CA certificates | M | |
| 4.2.1.11 | **Name Constraints** | CA – O App - M | Restricts name space for all subject names in subsequent certificates in certification path. |
| | Critical | M | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Used only with CA certificates | M | |
| | Restrictions apply to subject DN | O | |
| | Restrictions apply to subject alternative names | O | |
| | Restrictions defined by permitted subtrees | O | |
| | Restrictions defined by excluded subtrees | O | |
| | Names appearing here are invalid regardless of permitted subtrees information | M | |
| | Syntax GeneralSubtree | M | |
| | base GeneralName | O | ref. 4.2.1.7 |
| | rfc822Name | O | |
| | "*" wildcard for host part of the name permitted | O | |
| | Constraint applies to PKCS #9 email attributes in subject DN when: | C | Legacy systems |
| | RFC 822 names are constrained | M | |
| | PKCS #9 email attributes present in subject DN | M | |
| | Subject alternative names not included | M | |
| | URI | O | |
| | "*" wildcard for host part of the name permitted | O | |
| | dNSName | O | |
| | "*" wildcard use permitted | O | |
| | directoryName | O | |
| | Apply restrictions to certificate subject field | M | |
| | Apply restrictions to subjectAltName extensions of type directoryName | M | |
| | x400Address | O | |
| | Apply restrictions to subjectAltName of type x400Address | M | |
| | otherName | O | UNSPECIFIED |
| | ediPartyName | O | UNSPECIFIED |
| | iPAddress | O | UNSPECIFIED |
| | registeredID | O | UNSPECIFIED |
| | minimum field is zero | M | Not used with any name forms |
| | maximum field is absent | M | Not used with any name forms |
| 4.2.1.12 | **Policy Constraints** | CA – O<br>App - M | Constrains path validation |
| | Used with CA certificates | O | |
| | Prohibit policy mapping | O | |
| | Value of inhibitPolicyMapping indicates number of additional certificates that may appear before further policy mapping is prohibited | M | |
| | NULL if requireExplicitPolicy present | M | |
| | Present if requireExplicitPolicy field NULL | M | |
| | Each certificate in the path contains an acceptable policy statement | O | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Acceptable policy identifier in subsequent certificates | M | |
| | Identifier of a user required policy | O | |
| | Identifier of a policy declared equivalent by policy mapping | O | |
| | Value of requireExplicitPolicy indicates number of additional certificates that may appear before another explicit policy | M | |
| | NULL if inhibitPolicyMapping present | M | |
| | Present if inhibitPolicyMapping field NULL | M | |
| | Application behavior on receipt of NULL policy constraint fields | O | UNSPECIFIED |
| | Critical | O | |
| | Syntax | M | |
| | requiredEXplicitPolicy [0] | O | |
| | SkipCerts INTEGER (0..MAX) | M | |
| | inhibitPolicyMapping [1] | O | |
| | SkipCerts INTEGER (0..MAX) | M | |
| 4.2.1.13 | **CRL Distribution Points OID ::= {id-ce 31}** | O | Identifies how CRL information is obtained. RECOMMENDED |
| | Non-Critical | O | |
| | SEQUENCE | M | |
| | distributionPointName CHOICE | O | |
| | fullName GeneralName | O | ref. 4.2.1.7 |
| | otherName | O | |
| | OID | M | |
| | related value | M | |
| | rfc822Name | O | |
| | IA5String | M | |
| | Wildcard characters prohibited | M | |
| | Host names only | M | |
| | dNSName | O | |
| | IA5String | M | |
| | Wildcard characters prohibited | M | |
| | Subject is a subnet or a collection of hosts | M | |
| | x400Address | O | |
| | ORAdress | M | |
| | dierctoryName | O | |
| | ediPartyName | O | |
| | nameAssigner | O | |
| | partyName | M | |
| | URI | O | Response to use of other protocol, relative pathname, or omission of host UNSPECIFIED |
| | Points to the current CRL for the associated reasons | M | Issued by cRLIssuer |
| | Absolute pathname to a host | M | |
| | ftp | O | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | anonymous | M | |
| | http | O | |
| | ldap | O | ref. RFC1778 |
| | mailto | O | ref. RFC1783 |
| | mail response containing CRL | M | |
| | IA5String | M | |
| | wildcard character prohibited | M | |
| | iPAddress | O | |
| | OCTET STRING | M | |
| | network byte order | M | ref. RFC791 |
| | each octet LSB is the LSB of the corresponding of network address | M | |
| | IPv4 length 4 octets | M | ref. RFC791 |
| | IPv6 length 16 octets | M | ref. RFC1883 |
| | registerID | O | |
| | OID | M | |
| | nameRelativetoCRLIssuer | O | |
| | X.501 type Name | M | |
| | RelativeDistinguishedName | M | |
| | AttributeType | M | |
| | DirectoryString | O | |
| | AttributeValue | M | |
| | printableString | C | FIRST CHOICE |
| | bmpString | C | SECOND CHOICE |
| | utf8String | C | THIRD CHOICE |
| | universalString | C | FOURTH CHOICE |
| | teletexString | O | USE UNSPECIFIED |
| | reasons | O | |
| | unused, value = 0 | O | |
| | keyCompromise, value = 1 | O | |
| | cACompromise, value = 2 | O | |
| | affiliationChanged, value = 3 | O | |
| | superseded, value = 4 | O | |
| | cessationofOperation, value = 5 | O | |
| | certificateHold, value = 6 | O | |
| | Field omitted | C | |
| | CRL includes revocations for all reasons | M | |
| | cRLIssuer GeneralName | O | ref. 4.2.1.7 |
| | otherName | O | |
| | OID | M | |
| | related value | M | |
| | rfc822Name IA5String | O | |
| | Wildcard characters prohibited | M | |
| | Host names only | M | |
| | dNSName IA5String | O | |
| | Wildcard characters prohibited | M | |
| | Subject is a subnet or a collection of hosts | M | |
| | x400Address | O | |
| | ORAdress | M | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | dierctoryName | O | |
| | ediPartyName | O | |
| | nameAssigner | O | |
| | partyName | M | |
| | URI | O | Response to use of other protocol, relative pathname, or omission of host UNSPECIFIED |
| | Points to the cRLIssuer | M | |
| | Absolute pathname to a host | M | |
| | ftp | O | |
| | anonymous | M | |
| | http | O | |
| | ldap | O | ref. RFC1778 |
| | mailto | O | ref. RFC1783 |
| | mail response containing CRL | M | |
| | IA5String | M | |
| | wildcard character prohibited | M | |
| | iPAddress | O | |
| | OCTET STRING | M | |
| | network byte order | M | ref. RFC791 |
| | each octet LSB is the LSB of the corresponding of network address | M | |
| | IPv4 length 4 octets | M | ref. RFC791 |
| | IPv6 length 16 octets | M | ref. RFC1883 |
| | registerID | O | |
| | OID | M | |
| | Field omitted | C | |
| | CRL issued by the CA that issued the certificate | M | |
| 4.2.1.14 | **Extended Key Usage Field** | CA – O App - M | Indicates purposes that the public key can be used for in addition or in lieu of the basic purpose stated in the Key Usage Extension Field (4.2.1.3) |
| | Private key purposes | O | |
| | OIDs identify key purposes | M | ref. ITU-T Rec. X.660 or ISO/IEC 9834-1 |
| | Critical | O | Determined by certificate user |
| | Only one purpose permitted | M | |
| | Critical key usage field extension present | O | ref. 4.2.1.3 |
| | Process both fields | M | |
| | Certificate use consistent with both fields | M | |
| | Purposes inconsistent, certificate is rejected | M | |
| | Non-Critical | O | Determined by certificate user |
| | Multiple purposes permitted | O | |
| | Use to find a key/certificate from multiple | O | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Key usage unrestricted | M | |
| | Applications can require purpose be indicated | O | |
| | ExtKeyUsageSyntax SEQUENCE SIZE (1..MAX) OF | M | |
| | KeyPurposeId | M | |
| | TLS Web server authentication purpose | O | |
| | OID ::= {id-kp 1} | M | |
| | digitalSignature key usage bit | O | |
| | keyEncipherment key usage bit | O | |
| | keyAgreement key usage bit | O | |
| | TLS Web client authentication purpose | O | |
| | OID ::= {id-kp 2} | M | |
| | digitalSignature key usage bit | O | |
| | keyAgreement key usage bit | O | |
| | Signing of downloadable executable code purpose | O | |
| | OID ::= {id-kp 3} | M | |
| | digitalSignature key usage bit | O | |
| | E-mail protection purpose | O | |
| | OID ::= {id-kp 4} | M | |
| | digitalSignature key usage bit | O | |
| | nonRepudiation key usage bit | O | |
| | keyEncipherment key usage bit | O | |
| | keyAgreement key usage bit | O | |
| | IP security end system purpose | O | |
| | OID ::= {id-kp 5} | M | |
| | digitalSignature key usage bit | O | |
| | keyEncipherment key usage bit | O | |
| | keyAgreement key usage bit | O | |
| | IP security tunnel termination purpose | O | |
| | OID ::= {id-kp 6} | M | |
| | digitalSignature key usage bit | O | |
| | keyEncipherment key usage bit | O | |
| | keyAgreement key usage bit | O | |
| | IP security user | O | |
| | OID ::= {id-kp 7} | M | |
| | digitalSignature key usage bit | O | |
| | keyEncipherment key usage bit | O | |
| | keyAgreement key usage bit | O | |
| | Bind time to the hash of an object | O | |
| | OID ::= {id-kp 8} | M | |
| | digitalSignature key usage bit | O | |
| | nonRepudiation key usage bit | O | |
| 4.2.2 | **PRIVATE INTERNET EXTENSIONS** | O | |
| | Future extensions defined under id-pe arc | M | |
| 4.2.2.1 | **Authority Information Access** | O | Indicates how to access CA information and services |
| | CRLs location not given in this extension | M | ref. 4.2.1.13 |
| | Present in subject certificates | O | |
| | Present in CA certificates | O | |
| | Non-critical | M | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | AuthorityInfoAccessSyntax ::= SEQUENCE SIZE (1..MAX) OF | M | Describes the location and format of additional CA information |
| | AcessDescription ::= SEQUENCE | M | |
| | accessMethod | M | |
| | ocsp | O | |
| | Syntax defined in OCSP | M | ref. [PKIXOCSP] |
| | accessLocation | M | |
| | On-line status server description | M | |
| | URI IA5String | M | |
| | Access protocol to obtain current certificate status for certificate w/ this extension | M | |
| | URI IA5String | M | |
| | caIssuers | O | Description of the superior CAs in the certification path to aid certificate users in reaching a trusted termination point |
| | Syntax defined in OCSP | M | ref. [PKIXOCSP] |
| | accessLocation | M | |
| | Referenced description server | M | |
| | URI IA5String | M | |
| | Access protocol to obtain referenced description | M | |
| | URI IA5String | M | |
| | Other access descriptors | O | TBD |
| | authorityInfoAccess in a PKCS #7 encapsulation | O | |
| | Attributes | M | Locate certificates automatically rather than include certificates directly ref. PKCS #9, X.520, X.501 |
| | Certificate retrieval mechanism | M | |
| | [PKIXOCSP] | M | |
| | [PKIXLDAP] | M | |
| | URI form | O | |
| | HTTP retrieval mechanism | M | |
| | Append a filename to URL | M | |
| | IA5String | M | |
| | Concatenation of | M | |
| | SHA1 (Issuer DN or certificate serial number) | M | |
| | hexadecimal number using digits and lowercase letters “a” through “f” | M | |
| | issuerAndSerialNumber | M | |
| | SignerInfo syntax of PKCS #7 | M | |
| | “.cer” | M | |
| | DER encoded certificate | M | |
| | Retrieve file of requested certificate | M | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Use authorityInfoAccess extension in retrieved certificate to complete a certificate path | M | |
| 5 | **CRL AND CRL EXTENSIONS** | M | |
| | A revocation or status mechanism exists | M | |
| | CRL mechanism | O | |
| | CA issues version 2 CRLs | M | |
| | nextUpdate field | M | ref. 5.1.2.5 |
| | Applications can process version 1 and 2 CRLS | M | |
| | Private Internet CRL extensions or entry extensions | O | UNSPECIFIED |
| 5.1 | **CRL FIELDS** | M | |
| | Data to be signed is ASN.1 DER encoded | M | ref. X.208 – 88, a TLV encoding for each element |
| 5.1.1 | **CertificateList** | M | |
| 5.1.1.1 | **tbsCertList** TBSCertList | M | ref. 5.1.2 |
| 5.1.1.2 | **signatureAlgorithm** | M | |
| | AlgorithmIdentifier | M | Algorithm used by CA to sign CertificateList |
| | algorithm OID | M | |
| | Supported signature algorithms | M | ref. 7.2, |
| | parameters NULL | M | |
| 5.1.1.3 | **signature** | M | |
| | CA generated | M | ref. 7.2 for details on each supported algorithm |
| | ASN.1 DER encoded TBSCertList is inputted into a one-way hash | M | |
| | Hash output is encrypted to form signed quantity | M | |
| | Signed quantity is ASN.1 encoded as a BIT STRING | M | |
| 5.1.2 | **TBSCertList** | M | |
| 5.1.2.1 | **Version** | C | ref. 4.1.2.1 |
| | 509v1 CRLs - Neither CRL extensions nor CRL entry extensions are present, omit field | O | |
| | 509v2 CRLs - CRL extensions are present, value = 1 | M | |
| 5.1.2.2 | **Signature** | M | |
| | AlgorithmIdentifier | M | Algorithm used by CA to sign CRL |
| | algorithm OID | M | |
| | Supported signature algorithms | M | ref. 7.2, |
| | Value same as signatureAlgorithm | M | ref. 5.1.1.2 |
| | parameters NULL | M | |
| 5.1.2.3 | **Issuer Name** | M | Identifies entity who has signed and issued CRL |
| | X.500 distinguished name | O | ref. 4.1.2.4 |
| | issuerAltName extension present | O | |
| | X.501 type Name | M | |
| | RelativeDistinguishedName | M | |
| | AttributeType | M | ref. X.500 |
| | AttributeValue | M | ref. X.500 |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | DirectoryString | O | |
| | printableString | O | |
| | teletexString | C | |
| | bmpString | C | |
| | universalString | C | |
| | NULL | O | |
| | issuerAltName extension present | M | |
| | Critical | M | |
| 5.1.2.4 | **This Update** | M | Issue date of the CRL |
| | thisUpdate Time | M | |
| | CAs use utcTime through 2049 | M | ref. 4.1.2.5.1 |
| | Values expressed in Zulu | M | |
| | Values include seconds | M | |
| | Interpretation of YY field by CRL users | M | |
| | >= 50 then 19YY | M | Shouldn't appear if CA conforms to specification |
| | < 49 then 20YY | M | |
| | CAs use generalTime 2050 or after | M | ref. 4.1.2.5.2 |
| | Values expressed in Zulu | M | |
| | Values include seconds | M | |
| | Values not include fractional seconds | M | |
| 5.1.2.5 | **Next Update** | M | Date by which the next CRL will be issued |
| | nextUpdate Time | M | |
| | CRL issued earlier than this date | O | |
| | CRL issued no later than this date | M | |
| | Behavior on receipt of NULL field | O | UNSPECIFIED |
| | CAs use utcTime through 2049 | M | ref. 4.1.2.5.1 |
| | Values expressed in Zulu | M | |
| | Values include seconds | M | |
| | Interpretation of YY field by CRL users | M | |
| | >= 50 then 19YY | M | Shouldn't appear if CA conforms to specification |
| | < 49 then 20YY | M | |
| | CAs use generalTime 2050 or after | M | ref. 4.1.2.5.2 |
| | Values expressed in Zulu | M | |
| | Values include seconds | M | |
| | Values not include fractional seconds | M | |
| 5.1.2.6 | **Revoked Certificates** | O | Listing of revoked certificates |
| | Use field if CA has revoked unexpired certificates | M | ref. 5.1.2 |
| | revokedCertificates SEQUENCE OF SEQUENCE | M | |
| | userCertificate | M | |
| | CertificateSerialNumber | M | ref. 4.1.2.2 Revoked certificates are named by their SN |
| | revocationDate | M | ref. 5.1.2.4 |
| | CAs use utcTime through 2049 | M | ref. 4.1.2.5.1 |
| | Values expressed in Zulu | M | |
| | Values include seconds | M | |
| | Interpretation of YY field by CRL users | M | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | >= 50 then 19YY | M | Shouldn't appear if CA conforms to specification |
| | < 49 then 20YY | M | |
| | CAs use generalTime 2050 or after | M | ref. 4.1.2.5.2 |
| | Values expressed in Zulu | M | |
| | Values include seconds | M | |
| | Values not include fractional seconds | M | |
| | crlEntryExtensions | O | ref. 5.3 |
| | If present, v2 extensions | M | |
| 5.1.2.7 | **Extensions** | O | |
| | crlExtensions EXPLICIT | M | |
| | Use only if version number is 2 | M | ref. 5.1.2.1 |
| | Sequence of CRL extensions | M | ref. 5.2 |
| 5.2 | **CRL EXTENSIONS** | M | ref. ANSI X9.55, ISO X.509 |
| | CRL validation fails on encountering unrecognized critical CRL extension | M | |
| | Ignore unrecognized non-critical CRL extensions | O | |
| | Definition of private CRL extensions | O | |
| | Restrict use of critical private CRL extensions | M | |
| 5.2.1 | **Authority Key Identifier** | O | RECOMMENDED |
| | Non-critical | M | |
| | Use when issuer has multiple signing keys | O | |
| | Syntax | M | ref. 4.2.1.1 |
| | keyIdentifier OCTET STRING | O | RECOMMENDED |
| | Subject key identifier in CRL signer's certificate | M | |
| | authorityCertIssuer | O | |
| | NULL field | C | |
| | keyIdentifier present | M | |
| | Present | C | |
| | authorityCertSerialNumber also present | M | |
| | Syntax | M | ref. 4.2.1.7 |
| | otherName OID | O | |
| | related value EXPLICIT | M | |
| | Define by OID | M | |
| | rfc822Name IA5String | O | |
| | Wildcard character prohibited | M | |
| | dNSName IA5String | O | |
| | Wildcard character prohibited | M | |
| | x400Address ORAdress | O | |
| | directoryName | O | ref. 4.1.2.4 |
| | X.500 distinguished name | O | |
| | X.501 type Name | M | |
| | RelativeDistinguishedName | M | |
| | AttributeType OID | M | |
| | AttributeValue | M | |
| | PrintableString | C | FIRST CHOICE |
| | BMPString | C | SECOND CHOICE |
| | UTF8String | C | THIRD CHOICE |
| | UniversalString | C | FOURTH CHOICE |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | TeletexString | O | Unspecified |
| | ediPartyName | O | |
| | nameAssigner | O | |
| | PrintableString | O | |
| | BMPString | O | |
| | UTF8String | O | |
| | UniversalString | O | |
| | TeletexString | O | |
| | partyName | M | |
| | PrintableString | O | |
| | BMPString | O | |
| | UTF8String | O | |
| | UniversalString | O | |
| | TeletexString | O | |
| | URI IA5String | O | |
| | Points to a sequence of certificates issued by a CA | M | |
| | Absolute pathname to a host | M | No |
| | ftp | O | |
| | anonymous | M | |
| | http | O | |
| | ldap | O | RFC1778 |
| | mailto | O | RFC1783 |
| | mail response to sender containing subject's certificate | M | |
| | Behavior on omission of host. | O | None specified |
| | Behavior on provision of relative pathname | O | None specified |
| | Behavior on provision of other schemes | O | None specified |
| | Wildcard character prohibited | M | |
| | iPAddress OCTET STRING | O | |
| | network byte order | M | RFC791 |
| | each octet LSB is the LSB of the corresponding of network address | M | |
| | IPv4 length 4 octets | M | RFC791 |
| | IPv6 length 16 octets | M | RFC1883 |
| | registerID OID | O | |
| | authorityCertSerialNumber INTEGER | O | |
| | NULL field | C | |
| | keyIdentifier present | M | |
| | Present | C | |
| | authorityCertIssuer also present | M | |
| 5.2.2 | **Issuer Alternative Name** | O | |
| | Applications support reception of CRL with this extension marked critical | M | |
| | CA support of issuerAltName | M | ref. 4.2.1.8 |
| | Only alternative name form present | O | |
| | Issuer DN is NULL | O | RECOMMENDED |
| | Extension is used | O | RECOMMENDED |
| | Client behavior on encountering empty field | O | None Specified |
| | Extension is critical | M | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | A name can appear in multiple forms for each instance | O | |
| | Syntax | M | ref. 4.2.1.7 |
| | otherName OID | O | |
| | related value EXPLICIT | M | |
| | Define by OID | M | |
| | rfc822Name IA5String | O | |
| | Wildcard character prohibited | M | |
| | dNSName IA5String | O | |
| | Wildcard character prohibited | M | |
| | x400Address ORAdress | O | |
| | directoryName | O | ref. 4.1.2.4 |
| | X.500 distinguished name | O | |
| | X.501 type Name | M | |
| | RelativeDistinguishedName | M | |
| | AttributeType OID | M | |
| | AttributeValue | M | |
| | DirectoryString | O | |
| | PrintableString | C | FIRST CHOICE |
| | BMPString | C | SECOND CHOICE |
| | UTF8String | C | THIRD CHOICE |
| | UniversalString | C | FOURTH CHOICE |
| | TeletexString | O | USE UNSPECIFIED |
| | ediPartyName | O | |
| | nameAssigner | O | |
| | PrintableString | O | |
| | BMPString | O | |
| | UTF8String | O | |
| | UniversalString | O | |
| | TeletexString | O | |
| | partyName | M | |
| | PrintableString | O | |
| | BMPString | O | |
| | UTF8String | O | |
| | UniversalString | O | |
| | TeletexString | O | |
| | URI IA5String | O | |
| | Points to a sequence of certificates issued by a CA | M | |
| | Absolute pathname to a host | M | No |
| | ftp | O | |
| | anonymous | M | |
| | http | O | |
| | ldap | O | RFC1778 |
| | mailto | O | RFC1783 |
| | mail response to sender containing subject's certificate | M | |
| | Behavior on omission of host. | O | None specified |
| | Behavior on provision of relative pathname | O | None specified |
| | Behavior on provision of other schemes | O | None specified |
| | Wildcard character prohibited | M | |
| | iPAddress OCTET STRING | O | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | network byte order | M | RFC791 |
| | each octet LSB is the LSB of the corresponding of network address | M | |
| | IPv4 length 4 octets | M | RFC791 |
| | IPv6 length 16 octets | M | RFC1883 |
| | registerID OID | O | |
| 5.2.3 | **CRL Number** | M | |
| | Non-critical | M | |
| | Monotonically increasing sequence number | M | |
| | Used to determine most current CRL | M | |
| | A separate sequence for each specific CA X.500 directory entry or CRL distribution point | M | |
| | Issuing CAs include in all CRLs | M | |
| 5.2.4 | **Issuing Distribution Point** | O | |
| | Critical | M | |
| | Applications support reception of CRL with extension | M | |
| | CRL stored in X.500 directory | C | |
| | Stored in directory entry for CRL distribution point | M | |
| | CRL distribution point has a separate entry from CA | O | |
| | Partition of CRL distribution points | O | |
| | Separate distribution point for revocations with keyCompromise code | M | |
| | Use onlySomeReasons to associate reason codes with distribution point | M | |
| | onlySomeReasons absent | C | |
| | Distribution point contains revocations for all reasons | M | |
| | Syntax | M | |
| | distributionPoint | O | |
| | DistributionPointName | M | ref. 4.2.1.13 |
| | URL | O | |
| | Points to most current CRL | M | |
| | URI | M | |
| | Absolute pathname | M | |
| | Specify host | M | |
| | ftp | O | |
| | http | O | |
| | mailto | O | RFC1738 |
| | ldap | O | RFC1778 |
| | onlyContainsUserCerts BOOLEAN | M | |
| | DEFAULT FALSE | M | |
| | onlyContainsCACerts BOOLEAN | M | |
| | DEFAULT FALSE | M | |
| | onlySomeReasons | O | |
| | ReasonFlags BIT STRING | M | ref. 4.2.1.13 |
| | unused, value = 0 | O | |
| | CRL includes revocations for all reasons | M | |
| | keyCompromise, value = 1 | O | |
| | cACompromise, value = 2 | O | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | affiliationChanged, value = 3 | O | |
| | superseded, value = 4 | O | |
| | cessationofOperation, value = 5 | O | |
| | certificateHold, value = 6 | O | |
| | indirectCRL BOOLEAN | M | |
| | DEFAULT FALSE | M | |
| 5.2.5 | **Delta CRL Indicator** | O | |
| | Critical | M | |
| | Applications support reception of CRL with extension | M | |
| | Update local database on reception | M | |
| | CA concurrently issues full CRL | M | |
| | BaseCRLNumber is the cRLNumber of the base CRL (starting point for delta-CRLs) | M | |
| | delta-CRL contains changes from base CRL to CRL concurrently issued | M | |
| | The same CRLNumber for both the delta-CRL and the concurrent CRL | M | |
| | BaseCRLNumber of received delta-CRL is more than one greater then the BaseCRLNumber of the last received delta-CRL | C | |
| | CRL database unusable | M | |
| | Syntax | M | |
| | CRLNumber | M | ref. 5.2.3 |
| 5.2.6 | **Certificate Issuer** | O | |
| | indirectCRL indicator set TRUE | C | ref. 5.2.4 |
| | Certificate issuer extension not present on first entry | C | |
| | Default to CRL issuer | M | |
| | Certificate issuer extension not present on subsequent entries | C | |
| | Default to certificate issuer for preceding entry | M | |
| | CA uses extension when issuing CRLs | O | |
| | Mark extension critical | M | |
| | Applications support reception of CRL with extension | M | |
| | Syntax | M | |
| | GeneralNames | M | ref. 4.2.1.7 |
| 5.3 | **CRL ENTRY EXTENSIONS** | O | ref. ISO X.509, ANSI X9.55 |
| | CRL validation fails on encountering unrecognized critical CRL entry extension | M | |
| | Ignore unrecognized non-critical CRL entry extensions | O | |
| | Definition of private CRL entry extensions | O | |
| | Designate non-critical | O | |
| | Designate critical | O | |
| | Restrict use of critical private CRL extensions outside of defining community | M | |
| | Support by CAs and applications | O | |
| 5.3.1 | **Reason Code** | O | RECOMMENDED |
| | Non-critical | M | |
| | Syntax | M | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | unspecified (0) | O | |
| | CRL entry extension absent rather than use unspecified | O | |
| | keyCompromise (1) | O | |
| | cACompromise (2) | O | |
| | affiliationChanged (3) | O | |
| | superseded (4) | O | |
| | cessationOfOperation (5) | O | |
| | certificateHold (6) | O | |
| | removeFromCRL (7) | O | |
| 5.3.2 | **Hold Instruction Code** | O | RECOMMENDED |
| | Non-critical | M | |
| | Applications recognize holdinstruction-none | M | |
| | Treat as an absence of a hold instruction | M | |
| | Applications recognize holdinstruction-callissuer | M | |
| | Application call certificate issuer | O | |
| | Application reject certificate | O | |
| | Applications recognize holdinstruction-reject | M | |
| | Application reject certificate | M | |
| | Syntax | M | |
| | holdinstruction-none | O | NOT RECOMMENDED |
| | holdinstruction-callissuer | O | |
| | holdinstruction-reject | O | |
| 5.3.3 | **Invalidity Date** | O | RECOMMENDED |
| | Non-critical | M | |
| | Date private key was compromised or certificate became invalid | M | |
| | Earlier than CRL revocation date | O | |
| | Later than issue date of previously issued CRL | M | |
| | generalTime | M | ref. 4.1.2.5.2 |
| | Values expressed in Zulu | M | |
| | Values will include seconds | M | |
| 6 | **CERTIFICATE PATH VALIDATION** | | ref. Section 12.4.3 [X.509]. Verifies the binding between subject DN and subject public key, limited by the constraints which are specified in the certificates that comprise the path. |
| | Certification path processing logic verifies subject DN binding to subject public key | M | |
| | Non-specified algorithms must be functionally equivalent | M | |
| | Algorithm for validating certification paths | O | |
| | “Most-trusted CA” at beginning of path | M | |
| | Path validation procedure the same regardless of policy establishing “most-trusted CA” | M | |
| | “Self-signed” certificate contains public key | M | |
| | Certificate in path does not use subject identifier field | M | |
| | If present the certificate is still processed | M | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Certificate in path does not use unique identifier field | M | |
| | If present the certificate is still processed | M | |
| | Certificate in path does not use private critical extensions | M | |
| | If present the certificate is still processed | M | |
| | Sequence of certificates | M | |
| | For all certificates, the subject of a certificate in the sequence, is the issuer of the next certificate in the sequence | M | |
| | The first certificate in the sequence is the self-signed certificate | M | |
| | The last certificate in the sequence is the end entity certificate | M | |
| | Inputs | M | |
| | The certificate path has a defined length | M | |
| | An identifier to an acceptable certificate policy is available | M | |
| | Policy identifiers each comprising a sequence of policy element identifiers | O | |
| | Special value “any-policy” | O | |
| | Current date/time is available | M | |
| | Resulting state variables | M | |
| | Acceptable Policy Set | M | Certificate policy identifiers to recognized polices or the equivalent through policy mapping |
| | Initial value is “any-policy” | M | |
| | Constrained subtrees | M | A set of root names and subtrees within which ALL subject names of subsequent certificates may appear |
| | Initial value is “unbounded” | M | |
| | Excluded subtrees | M | A set of root names and subtrees within which NO subject names of subsequent certificates may appear |
| | Initial value is “empty” | M | |
| | Explicit policy | M | ref. 4.2.1.12 |
| | Identifies first certificate in path where an explicit policy identifier is required | M | |
| | Once set this requirement can not be removed by a later certificate | M | |
| | Integer | M | |
| | Initial value n+1 | M | |
| | Decrement only | M | |
| | Policy mapping | M | ref. 4.2.1.6 |
| | Identifies last certificate in path on which policy mapping is applied | M | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Once set this requirement can not be removed by a later certificate | M | |
| | Integer | M | |
| | Initial value n+1 | M | |
| | Decrement only | M | |
| | Certificate processing | M | |
| | Performed sequentially | M | |
| | State variables from processing a certificate affect the subsequent certificate | M | |
| | Verify basic certificate information | M | |
| | Certificate was signed by subject public key from previous certificate | M | |
| | In the case of the self-signed certificate | M | |
| | Omit the step | O | |
| | Use same certificate subject public key | O | |
| | Certificate is not expired | M | |
| | Private key usage period is satisfied | O | NOT RECOMMENDED |
| | Certificate is not revoked | M | |
| | Subject and issuer names chain correctly | M | |
| | Name field empty | O | |
| | Use critical subjectAltNames and issuerAltNames | M | |
| | Failure terminates path processing | M | |
| | Basic certificate information fault returned | M | |
| | Verify subject name vice constrained subtrees state variables | M | |
| | Name field empty | O | |
| | Use critical subjectAltNames | M | |
| | Failure terminates path processing | M | |
| | Subject name not present in constrained subtrees fault returned | M | |
| | Verify subject name vice excluded subtrees state variables | M | |
| | Name field empty | O | |
| | Use critical subjectAltNames | M | |
| | Failure terminates path processing | M | |
| | Subject name not present in excluded subtrees fault returned | M | |
| | Verify that policy information is consistent with the initial policy set | M | |
| | Explicit policy state variable is required | O | |
| | Certificate policy identifier part of initial policy set | M | |
| | Policy mapping state variable is set | O | |
| | Can not map the policy identifier | M | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Failure terminates path processing | M | |
| | Policy information inconsistent with the initial policy set fault returned | M | |
| | Verify that policy information is consistent with the acceptable policy set | M | |
| | Certificate policies extension marked critical | O | |
| | Non-NULL intersection of the OIDs in the certificate policies extension and the acceptable policy set | M | ref. 4.2.1.5 |
| | Intersection of the OIDs in the certificate policies extension and the acceptable policy set is assigned as the new value of the acceptable policy set | M | |
| | Failure terminates path processing | M | |
| | Policy information inconsistent with the acceptable policy set fault returned | M | |
| | Verify that the intersection of the set of acceptable policy identifiers and the set of initial policy identifiers is non-NULL | M | |
| | Failure terminates path processing | M | |
| | NULL intersection of acceptable policy set and initial policy set fault returned | M | |
| | Recognize and process any other critical extensions present | M | |
| | Does not apply to end entity certificate | M | |
| | Verify that the certificate is CA certificate | M | |
| | As specified in basicConstraints extension | O | ref. 4.2.1.10 |
| | As verified out-of-band | O | |
| | Does not apply to end entity certificate | M | |
| | Failure terminates path processing | M | |
| | Certificate is not a CA certificate fault returned | M | |
| | permittedSubtrees restriction present | C | ref. 4.2.1.11 |
| | Set constrained subtrees state variable to intersection of its previous value and the value in the nameConstraints extension field | M | |
| | Does not apply to end entity certificate | M | |
| | excludedSubtrees restriction present | C | ref. 4.2.1.11 |
| | Set excluded subtrees state variable to the union of its previous value and the value in the nameConstraints extension field | M | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Does not apply to end entity certificate | M | |
| | Policy constraints extension present | C | ref. 4.2.1.12 |
| | requireExplicitPolicy present | C | |
| | Set explicit policy state variable to the lesser of either | M | |
| | Its current value | O | |
| | The sum of requireExplicitPolicy value and the current certificate sequence value | O | |
| | inhibitPolicyMapping present | C | |
| | Set policy mapping state variable to the lesser of either | M | |
| | Its current value | O | |
| | The sum of inhibitPolicyMapping value and the current certificate sequence value | O | |
| | Does not apply to end entity certificate | M | |
| | Processing succeeds with end-entity certificate | C | |
| | Procedure terminates | M | |
| | Success indication returned | M | |
| | Set of all policy qualifier values encountered returned | M | ref. 4.2.1.5 |
| | Extensions to specified path processing | O | |
| | PEM functionality | O | |
| | Input list of PCA names and indicator of the PCA's expected position in the certification path | M | |
| | At PCA location compare CA name to list | M | |
| | Recognized PCA name found | C | |
| | Set SubordinateToCA constraint for remainder of processing | M | |
| | No recognized PCA name found | C | |
| | Certification path cannot be validated on basis of identified policies | C | |
| | Certification path invalid | M | |
| | Path validation module provided a set of self-signed certificates | O | |
| | Any of the self-signed certificates starts valid path | M | |
| | Path validation module incorporates local security policy and requirements | M | |
| 7 | **Algorithm Support** | | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | Use of cryptographic algorithms or algorithm identifiers specified | O | |
| | Conformance when used | M | |
| 7.1 | **One-way Hash Functions** | M | |
| 7.1.1 | **MD2 One-way Hash Function** | O | ref. RFC1319<br>NOT RECOMMENDED |
| | Use with PEM certificates | O | |
| | Use to verify existing signatures | O | |
| | Checksum operation | M | |
| 7.1.2 | **MD5 One-way Hash Function** | O | ref. RFC1321<br>NOT RECOMMENDED |
| | Use to verify existing signatures | O | |
| 7.1.3 | **SHA-1 One-way Hash Function** | O | ref. FIPS 180-1<br>RECOMMENDED |
| | Use with RSA signature algorithms | M | |
| | Use with DSA signature algorithms | M | |
| 7.2 | **Signature Algorithms** | M | |
| | Use algorithm object identifiers specified in signatureAlgorithm field | M | ref. 4.1.1.2, 5.1.1.2 |
| | Use signature algorithms with one-way hash functions | M | ref. 7.1 |
| 7.2.1 | **RSA Signature Algorithm** | O | |
| | Combined with MD2 | O | ref. PKCS#1 |
| | md2WithRSAEncryption OID | M | |
| | Place OID in signature field | M | ref. 4.1.1.3, 5.1.1.3 |
| | Combined with MD5 | O | ref. PKCS#1 |
| | md5WithRSAEncryption OID | M | |
| | Place OID in signature field | M | ref. 4.1.1.3, 5.1.1.3 |
| | Combined with SHA-1 | O | ref. OIW SIA Pt. 12 |
| | Padding convention | M | ref. PKCS#1, sec. 8.1 |
| | sha1WithRSASignature OID | M | |
| | Place OID in signature field | M | ref. 4.1.1.3, 5.1.1.3 |
| | Data to be signed is ASN.1 encoded as an OCTET STRING | M | |
| | OCTET STRING is RSA encrypted to form the signature value | M | |
| | Signature value is ASN.1 encoded as a BIT STRING | M | |
| | MSB bit of signature value first bit in BIT STRING | M | |
| | Signature value is converted to OCTET STRING first | O | |
| 7.2.2 | **DSA Signature Algorithm** | O | ref. FIPS 186 |
| | Combined with SHA-1 | M | ref. OIW SIA Pt. 12 |
| | id-dsa-with-sha1 OID | M | |
| | Appears in certificate SubjectPublicKeyInfo field | O | ref. 4.1.2.7 |
| | DSA parameters applied to signature verification | M | |
| | AlgorithmIdentifier field of SubjectPublicKeyInfo has NULL parameters | C | ref. 7.3 |
| | CA signed subject certificate using DSA | O | |
| | Certificate issuer's parameters apply to subject's DSA key | M | |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | CA signed subject certificate using non-DSA algorithm | O | |
| | Certificate not valid | M | |
| | ASN.1 encode DSA generated “r” and “s” values for transfer | M | |
| 7.3 | **Subject Public Key Algorithm** | M | |
| | CAs use identified OIDs and parameters | M | |
| | Applications supporting algorithm recognize its OID | M | |
| 7.3.1 | **RSA Keys** | O | |
| | rsaEncryption OID | M | |
| | OID used in the algorithm field of a value of type AlgorithmIdentifier | M | ref. 4.1.2.7 |
| | Parameters of a value of type AlgorithmIdentifier NULL | M | ref. 4.1.2.7 |
| | RSA public key encoded using ASN.1 type RSAPublicKey | M | |
| | Value of DER encoded RSAPublicKey s BIT STRING subjectPublicKey | M | |
| | OID used in public key certificate for RSA signature keys | O | |
| | Indicate usage in key usage field | O | ref. 4.2.1.3 |
| | OID used in public key certificate for RSA encryption keys | O | |
| | Indicate usage in key usage field | O | ref. 4.2.1.3 |
| | Single public key for both RSA signature and encryption | O | NOT RECOMMENDED |
| | keyUsage extension present in end entity RSA public key certificate | C | |
| | digitalSignature | O | |
| | nonRepudiation | O | |
| | keyEncipherment | O | |
| | dataEncipherment | O | |
| | keyUsage extension present in CA RSA public key certificate | C | |
| | digitalSignature | O | |
| | nonRepudiation | O | |
| | keyEncipherment | O | |
| | dataEncipherment | O | |
| | keyCertSign | O | |
| | keyEncipherment absent | O | RECOMMENDED |
| | dataEncipherment absent | O | RECOMMENDED |
| | cRLSign | O | |
| | keyEncipherment absent | O | RECOMMENDED |
| | dataEncipherment absent | O | RECOMMENDED |
| 7.3.2 | **Diffie-Hellman Key Exchange** | O | |
| | dhpublicnumber OID | M | ANSI X9.42 |
| | OID used in the algorithm field of a value of type AlgorithmIdentifier | M | ref. 4.1.2.7 |
| | Parameters field of a value of type AlgorithmIdentifier contains ASN.1 type DHParameter | M | ref. 4.1.2.7 |

| SECTION | FEATURE | STATUS | REMARKS |
|---|---|---|---|
| | ASN.1 encode DH public key as an INTEGER for contents of subjectPublicKey component of SubjectPublicKeyInfo field | M | |
| | keyUsage extension present in a DH public key certificate | C | |
| | keyAgreement | O | |
| | encipherOnly | O | |
| | decipherOnly not present | M | |
| | decipherOnly | O | |
| | encipherOnly not present | M | |
| 7.3.3 | **DSA Signature Keys** | O | |
| | id-dsa OID | M | |
| | Algorithm optional parameters (p, q, g) omitted | C | |
| | Parameters field of a value of type AlgorithmIdentifier contains NULL | M | ref. 4.1.2.7 |
| | Algorithm parameters other then those related to DSA are present in the AlgorithmIdentifier field of SubjectPublicKeyInfo | C | |
| | CA signed subject certificate using DSA | O | |
| | Certificate issuer's DSA parameters apply to subject's DSA key | M | |
| | CA signed subject certificate using non-DSA algorithm | O | |
| | Subject's DSA parameters distributed by other means | M | |
| | AlgorithmIdentifier field of SubjectPublicKeyInfo has NULL parameters | C | |
| | CA signed subject certificate using DSA | O | |
| | Certificate issuer's DSA parameters apply to subject's DSA key | M | |
| | CA signed subject certificate using non-DSA algorithm | O | |
| | Certificate not valid | M | |
| | ASN.1 encode DSA generated "r" and "s" values for transfer as BIT STRING | M | |
| | ASN.1 encoded DSA public key as INTEGER are contents for subjectPublicKey BIT STRING in SubjectPublicKeyInfo field | M | |
| | keyUsage extension present in end entity DSA public key certificate | C | |
| | digitalSignature | O | |
| | nonRepudiation | O | |
| | keyUsage extension present in CA DSA public key certificate | C | |
| | digitalSignature | O | |
| | nonRepudiation | O | |
| | keyCertSign | O | |
| | cRLSign | O | |

Document Point of Contact:

Defense Information Systems Agency
ATTN: JIEO-JEBBC (Gregor D. Scott)
Ft. Monmouth, NJ 07703-5613
USA
Voice: 732-427-6856
Fax: 732-532-0853
Email: scottg@ftm.disa.mil